

Exhibit 2 to the Complaint.

**U.S. Patent No. US 8,265,089 v. Imperva
Claims 7 and 20 Exemplary**

Exhibit 2 to the Complaint.

1. Claim Chart

Claim	Analysis
<p>[7.P] A gateway computer for use in a computer communication network system, the gateway computer comprising a non-transient software storage device with the following software encoded therein: a gateway module and an enhanced requesting module;</p>	<p>Imperva (“Company”) makes, uses, sells and/or offers to sell a gateway computer for use in a computer communication network system, the gateway computer comprising a non-transient software storage device with the following software encoded therein: a gateway module and an enhanced requesting module.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, Company provides an Incapsula distributed denial-of-service (DDoS) protection service, that uses an Imperva Global Network to protect from DDoS attackers. Further, the network includes a multi-function point-of-presence (PoP), where each PoP is equipped with multiple Behemoth 2 (“gateway computer”) units to prevent DDoS attacks.</p> <p>Furthermore, the DDoS protection service which uses the Behemoth 2, protects various online assets such as Websites, DNS servers, SMTP servers, and any other IP-based application (“computer communication network system”). Behemoth 2 includes an Alta switch in combination with a CPU, where some part of the software in the Alta switch performs the functioning of the gateway module while another part of the software performs the functioning of the enhanced requesting module in the process of DDoS protection.</p>

Exhibit 2 to the Complaint.

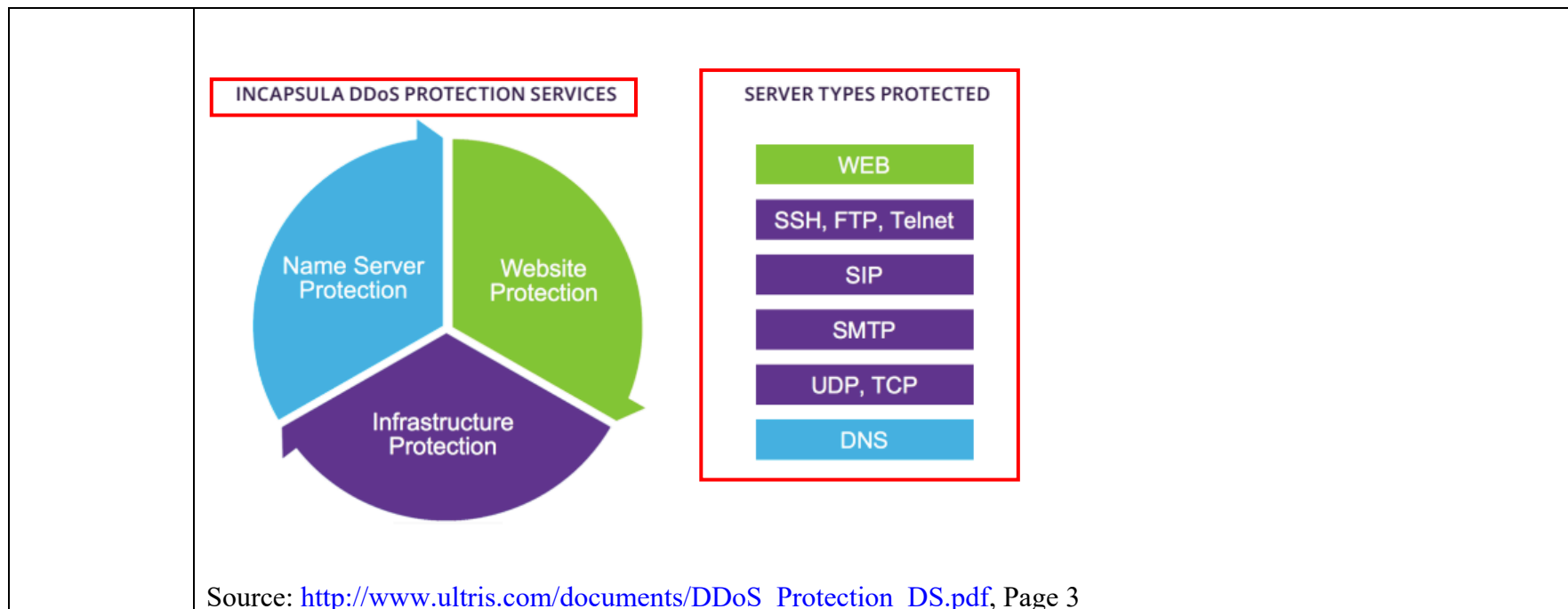


Exhibit 2 to the Complaint.

Incapsula Global Network

Unlike other services where DDoS was added to an existing content delivery network or web application firewall appliance, Incapsula designed a DDoS protection network from the ground up as an integral component of our comprehensive security and web acceleration solution. The Incapsula network fights the power of distributed attackers with an even greater distributed global defense. As the DDoS threat grows, so does the power of the Incapsula network. At the core of our network architecture is the multi-function PoP, distributed globally at strategic locations and served by major transit and hosting providers to ensure we remain close to your origin servers and end users. At the center of our DDoS mitigation capability is a purpose-built appliance that can manage up to 440 Gbps of traffic or 650 Mpps (millions of packets per second) – in fact, we call this The Behemoth. Each PoP is equipped with multiple Behemoths as well as WAF, bot protection, caching and load balancing services. The Incapsula network of PoPs continues to grow and can be seen on the [Incapsula network map](#).

Source: http://www.ultris.com/documents/DDoS_Protection_DS.pdf, Page 7

DDoS Protection for Networks can be used to protect any online asset such as websites, DNS servers, SMTP servers and any other IP based application. This service leverages Imperva's multi-terabit network capacity and packet processing capabilities to absorb and mitigate the largest and most sophisticated DDoS attacks.

DDoS Protection for Networks can be deployed as an always-on, on-demand or contingency solution, and can be combined with all Imperva Cloud Application Security services for extending protection and monitoring capabilities.

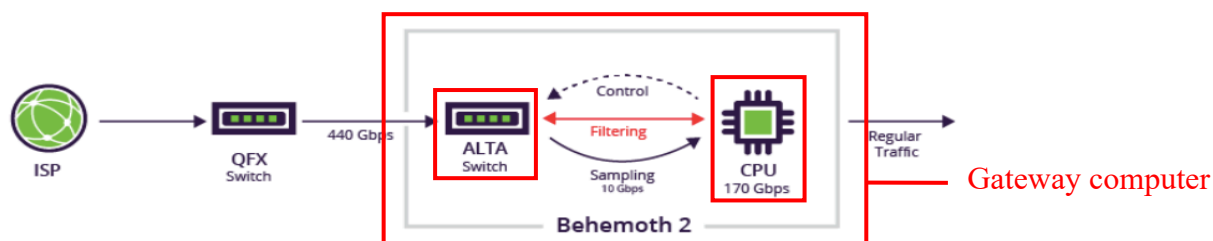
Source: <https://docs.imperva.com/bundle/cloud-application-security/page/introducing/network-ddos-protection.htm>

Exhibit 2 to the Complaint.



Behemoth 2

Source: <https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/> (annotated)



In the new configuration, all traffic to the PoP is redirected to Behemoth 2.

Source: <https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/> (annotated)

[7.1]
wherein:
the gateway
module is
structured,
programmed
and/or data-
communicati

Company provides a system wherein the gateway module is structured, programmed and/or data-communication-connected to receive a first MPDU from a connection-based network of the computer communication network system, to disaggregate the first MPDU into a plurality of smaller data units (DUs), and selectively communicate the first DU to a receiver-side connectionless network of the computer communication network system.

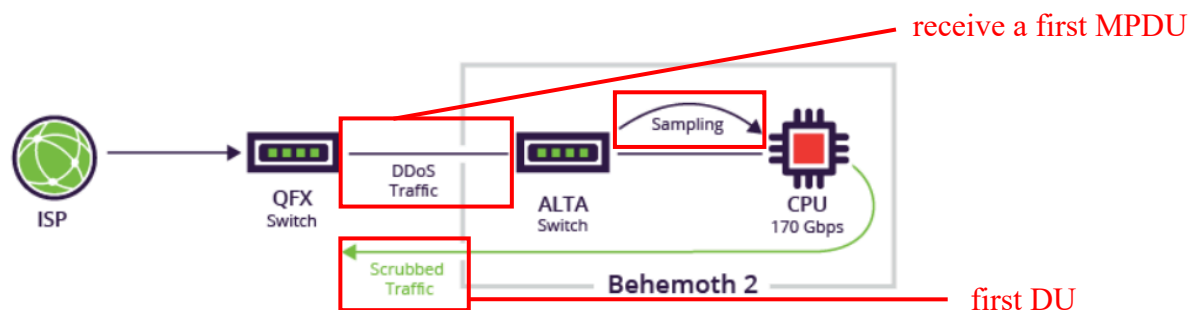
This element is infringed literally, or in the alternative, under the doctrine of equivalents.

Exhibit 2 to the Complaint.

on-connected to receive a first MPDU from a connection-based network of the computer communication network system, to disaggregate the first MPDU into a plurality of smaller data units (DUs), and selectively communicate the first DU to a receiver-side connectionless network of the computer communication network system; and

For example, the Alta switch receives all the traffic from the global network (“first MPDU”) and performs the function of sampling and scrubbing, where malicious packets are identified based on their header content, size, type, and point of origin. Therefore, it would be apparent to a person having ordinary skill in the art that the disaggregation of the first MPDU is done into a plurality of smaller data units (DUs) through the process of sampling and scrubbing.

Furthermore, after the sampling is done, the scrubbed traffic (“first DU”) is outputted from the CPU (“selectively communicate the first DU to a receiver-side connectionless network of the computer communication network system”).



Source: <https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/> (annotated)

- **Scrubbing**—an improvement on arbitrary sinkholing, scrubbing routes all ingress traffic through a security service. Malicious network packets are identified based on their header content, size, type, point of origin, etc. The challenge is to perform scrubbing at an inline rate without causing lag or otherwise impacting legitimate users.

Source: <https://www.imperva.com/learn/ddos/ddos-mitigation-services/>

Exhibit 2 to the Complaint.



In the new configuration, all traffic to the PoP is redirected to Behemoth 2.

As shown in the figure, all the traffic entering the PoP is diverted to Behemoth 2, which will then apply internal sampling for DDoS detection. It also controls the Alta switch to divert the traffic for software mitigation. Alternatively, the mitigation service can install rules on the switch to perform the packet drop in hardware.

Source: <https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/>

Exhibit 2 to the Complaint.

	<p>Single-stack speed, capacity, and accuracy</p> <p>Our high-capacity global network holds more than six Terabits per second (6 Tbps) of scrubbing capacity and can process more than 65 billion attack packets per second. This global network of 44+ points of presence (PoPs), each outfitted with a DDoS scrubbing center powered by proprietary Behemoth custom technology, cloud-based WAF, advanced bot mitigation services and more, acts as a software-defined mesh network for optimal performance. It scales as needed to absorb the largest attacks that can overwhelm legacy appliances. It also doesn't rely on a hybrid approach where failover to the cloud can mean the more persistent, small-scale attacks of today do damage before mitigation even starts. We incorporate crowdsourced learnings from emerging attack methods across our network, utilizing machine learning for the most up-to-date, accurate, and advanced protection.</p> <p>Source: https://www.imperva.com/resources/datasheets/Imperva_DDoS_Protection_20200730.pdf, Page 2</p>
<p>[7.2] the enhanced requesting module is structured, programmed and/or data-communication-connected to collect selected network protocol data from the first</p>	<p>Company provides a system wherein the enhanced requesting module is structured, programmed and/or data-communication-connected to collect selected network protocol data from the first MPDU, with the selected network protocol data including at least some network protocol data included in the first MPDU and not included in any of the plurality of DUs, and with the selected network protocol data relating exclusively to network protocols and including no data from any data payload(s) which may be present in the MPDU.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, the Alta switch performs the function of filtering where the DDoS traffic is filtered by identifying patterns that instantly distinguish between legitimate traffic and malicious traffic (“selected network protocol data including at least some network protocol data included in the first MPDU and not included in any of the plurality of DUs”) to generate the scrubbed traffic.</p>

Exhibit 2 to the Complaint.

MPDU, with the selected network protocol data including at least some network protocol data included in the first MPDU and not included in any of the plurality of DUs, and with the selected network protocol data relating exclusively to network protocols and including no data from any data payload(s) which may be present in the MPDU;

Furthermore, while sampling, different network-layer data packets such as UDP, and TCP are identified and mitigated to reduce the severity of the attack. Therefore, upon information and belief, mitigated UDP, and TCP data packets are the selected network protocol data relating exclusively to network protocols and including no data from any data payload(s) that may be present in the MPDU.



In the new configuration, all traffic to the PoP is redirected to Behemoth 2.

As shown in the figure, all the traffic entering the PoP is diverted to Behemoth 2, which will then apply internal sampling for DDoS detection. It also controls the Alta switch to divert the traffic for software mitigation. Alternatively, the mitigation service can install rules on the switch to perform the packet drop in hardware.

Source: <https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/>

Exhibit 2 to the Complaint.

3. Filtering—DDoS traffic is weeded out, usually by identifying patterns that instantly distinguish between legitimate traffic (i.e., humans, API calls and search engine bots) and malicious visitors. Responsiveness is a function of your being able to block an attack without interfering with your users' experience. The aim is for your solution to be completely transparent to site visitors.

Source: <https://www.imperva.com/learn/ddos/ddos-mitigation-services/>

How it Works

Dedicated hardware is deployed in each of our PoPs to perform the stream processing required in order to collect statistics at network speed. Probabilistic data structures are used in conjunction with deterministic counting in order to provide reliable top statistics.

Analytics data is based on a 1:40 sampling resolution for DDoS traffic and a 1:1 sampling ratio for clean traffic, and data is collected in 15-second buckets.

Source: <https://www.imperva.com/blog/archive/enhanced-infrastructure-ddos-protection-analytics-targeted-visibility-for-greater-accuracy/>

Exhibit 2 to the Complaint.

What is a PPS or Network Protocol DDoS Attack?

An internet protocol is a discrete set of rules for exchanging information across the internet. TCP/IP is one of the most well-known rules for exchanging requests and data. A bad actor can severely disrupt an online service by exploiting these rules.

Protocol attacks often work at layers 3 and 4 of the OSI model on network devices like routers. Because they are on the network layer, they are measured in packets per second (pps).

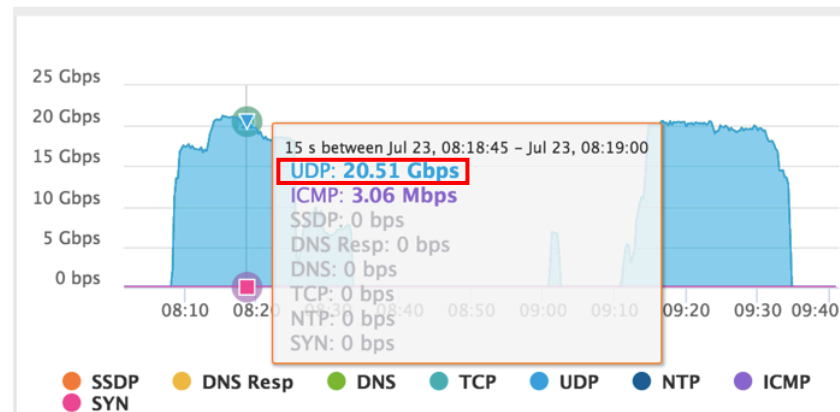
Below is a sampling of different network-layer DDoS attack types:

- UDP floods
- SYN floods
- NTP amplification
- DNS amplification
- SSDP amplification
- IP fragmentation
- SYN-ACK floods

Source: <https://www.imperva.com/learn/ddos/ddos-attacks/>

Exhibit 2 to the Complaint.

For a given range, we were able to display the size of the attack and the different attack vectors:



But other than the fact that we mitigated a lot of UDP traffic, it was impossible to dig deeper into the attack.

Source: <https://www.imperva.com/blog/archive/enhanced-infrastructure-ddos-protection-analytics-targeted-visibility-for-greater-accuracy/>

Support for any type of service

DDoS protection for networks supports any type of service, including TCP, UDP, SMTP, FTP, SSH, VoIP and proprietary or custom protocols.

Source: <https://www.imperva.com/products/infrastructure-ddos-protection-services/>

Exhibit 2 to the Complaint.

	<div> <h3>DDoS security policy</h3> <p>The traffic scrubbing that Imperva performs is based on a unique security policy that we define for each network range. The goal, of course, is to achieve the best granularity possible in order to minimize false positives and maximize mitigation.</p> <p>Imperva defines the security policy based on your traffic rates and patterns. When you first onboard your range to the DDoS for Networks service, we define an initial security policy according to our internal logic and the network information you provide in the scoping document. This information enables us to create an initial policy that allows a reasonable rate of traffic while blocking suspicious rates of traffic, until we have enough information to develop a more customized profile.</p> <p>After 7 days of traffic flow, the Imperva SD-SOC analyzes the data and automatically adjusts the security policy based on your network range's actual traffic patterns. Our Security Operations Center (SOC) reviews the policies as needed.</p> <h3>Mitigation process</h3> <p>The mitigation process built in to the Behemoth technology applies deep packet inspection combined with the application of advanced security rules and security challenges in order to identify malicious sources and/or content.</p> <p>Multiple mitigation steps are defined and evaluated independently for each traffic type, such as TCP, UDP, SYN, DNS, NTP, and so on.</p> <p>Each step is combined with thresholds in Kpps, Mbps, or both, in order to appropriately flag the traffic as malicious or legitimate. When the specified threshold is reached, the relevant mitigation step is activated. Mitigation steps are activated one at a time, as needed. Only the first and last steps are described here:</p> <p>Source: https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/security-policy.htm</p> </div>
[7.3] the enhanced requesting module is further	<p>Company provides a system wherein the enhanced requesting module is further structured, programmed and/or data-communication-connected to apply a first rule to the selected network protocol data collected by the enhanced requesting module.</p>

Exhibit 2 to the Complaint.

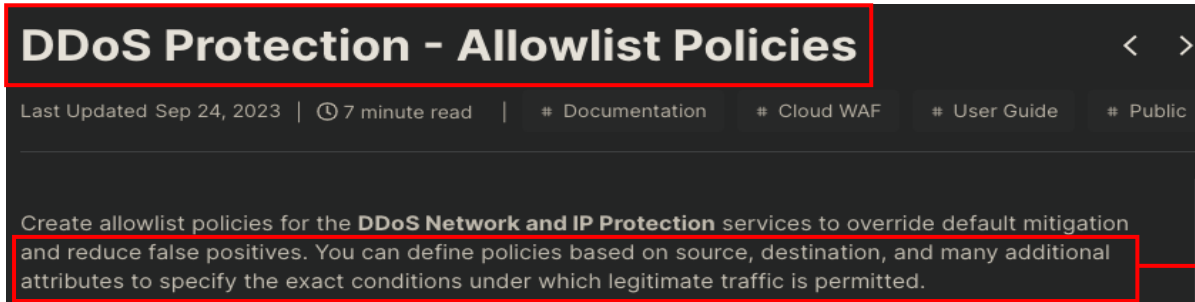
<p>structured, programmed and/or data-communication-connected to apply a first rule to the selected network protocol data collected by the enhanced requesting module; and</p>	<p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, the software in the Alta switch (“the enhanced requesting module”) applies the mitigation policies (“apply a first rule”) on the sampling data. The mitigation process built into the Behemoth technology applies deep packet inspection combined with the application of advanced security rules and security challenges to identify malicious sources and content. Multiple mitigation steps are defined and evaluated independently for each traffic type, such as TCP, UDP, SYN, DNS, and NTP.</p> <p>Flexibility: The Alta switching platform has greatly enhanced the TCAM capacity when compared to off-the-shelf switching platforms. This has let us greatly reduce false positives as we have a sufficient number of rules to divert specific IP addresses (/32) for mitigation rather than subnets (/24). Traffic which is not diverted for mitigation will flow uninterrupted inside the PoP.</p> <p>Source: https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/</p>  <p>Source: https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/network-protection-policies.htm (annotated)</p>
--	--

Exhibit 2 to the Complaint.

	<div data-bbox="420 280 802 323" data-label="Section-Header"> <h2>DDoS security policy</h2> </div> <div data-bbox="420 345 1625 446" data-label="Text"> <p>The traffic scrubbing that Imperva performs is based on a unique security policy that we define for each network range. The goal, of course, is to achieve the best granularity possible in order to minimize false positives and maximize mitigation.</p> </div> <div data-bbox="420 475 1642 644" data-label="Text"> <p>Imperva defines the security policy based on your traffic rates and patterns. When you first onboard your range to the DDoS for Networks service, we define an initial security policy according to our internal logic and the network information you provide in the scoping document. This information enables us to create an initial policy that allows a reasonable rate of traffic while blocking suspicious rates of traffic, until we have enough information to develop a more customized profile.</p> </div> <div data-bbox="420 672 1633 773" data-label="Text"> <p>After 7 days of traffic flow, the Imperva SD-SOC analyzes the data and automatically adjusts the security policy based on your network range's actual traffic patterns. Our Security Operations Center (SOC) reviews the policies as needed.</p> </div> <div data-bbox="420 812 764 852" data-label="Section-Header"> <h2>Mitigation process</h2> </div> <div data-bbox="420 875 1591 974" data-label="Text"> <p>The mitigation process built in to the Behemoth technology applies deep packet inspection combined with the application of advanced security rules and security challenges in order to identify malicious sources and/or content.</p> </div> <div data-bbox="420 1003 1585 1070" data-label="Text"> <p>Multiple mitigation steps are defined and evaluated independently for each traffic type, such as TCP, UDP, SYN, DNS, NTP, and so on.</p> </div> <div data-bbox="420 1097 1638 1198" data-label="Text"> <p>Each step is combined with thresholds in Kpps, Mbps, or both, in order to appropriately flag the traffic as malicious or legitimate. When the specified threshold is reached, the relevant mitigation step is activated. Mitigation steps are activated one at a time, as needed. Only the first and last steps are described here:</p> </div> <div data-bbox="405 1242 1797 1274" data-label="Text"> <p>Source: https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/security-policy.htm</p> </div>
--	--

Exhibit 2 to the Complaint.

	<div><div>Policy attributes</div><div>Use the following parameters to determine when the policy is applied.</div><div><div>Column </div><div>Filter results... </div></div><table><thead><tr><th>ATTRIBUTE NAME</th><th>DESCRIPTION</th><th>SUPPORTED OPERATORS</th><th>ALLOWED VALUES</th></tr></thead><tbody><tr><td>Filter</td><td>Filter</td><td>Filter</td><td>Filter</td></tr><tr><td>IP protocol number (ip.proto)</td><td>The protocol number of the IP packet.</td><td>==</td><td>0-255</td></tr><tr><td>Source IP (ip.src)</td><td>The source IP address of the packet.</td><td>==,>=,<=,>,<</td><td>Subnet or single IP</td></tr></tbody></table></div> <div>Source: https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/network-protection-policies.htm</div>	ATTRIBUTE NAME	DESCRIPTION	SUPPORTED OPERATORS	ALLOWED VALUES	Filter	Filter	Filter	Filter	IP protocol number (ip.proto)	The protocol number of the IP packet.	==	0-255	Source IP (ip.src)	The source IP address of the packet.	==,>=,<=,>,<	Subnet or single IP
ATTRIBUTE NAME	DESCRIPTION	SUPPORTED OPERATORS	ALLOWED VALUES														
Filter	Filter	Filter	Filter														
IP protocol number (ip.proto)	The protocol number of the IP packet.	==	0-255														
Source IP (ip.src)	The source IP address of the packet.	==,>=,<=,>,<	Subnet or single IP														
[7.4] the enhanced requesting module is further structured, programmed and/or data-communication-connected to selectively	<p>Company provides a system wherein the enhanced requesting module is further structured, programmed and/or data-communication-connected to selectively make a responsive reaction based, at least in part, upon the application of the first rule by the enhanced requesting module to the selected network protocol data.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, the Alta switch blocks the suspicious traffic (“responsive reaction”) based on the selected policies applied to the sampling data.</p>																

Exhibit 2 to the Complaint.

<p>make a responsive reaction based, at least in part, upon the application of the first rule by the enhanced requesting module to the selected network protocol data.</p>	<div data-bbox="411 269 1593 756"> <h3>DDoS security policy</h3> <p>The traffic scrubbing that Imperva performs is based on a unique security policy that we define for each network range. The goal, of course, is to achieve the best granularity possible in order to minimize false positives and maximize mitigation.</p> <p>Imperva defines the security policy based on your traffic rates and patterns. When you first onboard your range to the DDoS for Networks service, we define an initial security policy according to our internal logic and the network information you provide in the scoping document. This information enables us to create an initial policy that allows a reasonable rate of traffic while blocking suspicious rates of traffic, until we have enough information to develop a more customized profile.</p> <p>After 7 days of traffic flow, the Imperva SD-SOC analyzes the data and automatically adjusts the security policy based on your network range's actual traffic patterns. Our Security Operations Center (SOC) reviews the policies as needed.</p> </div> <p>Source: https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/security-policy.htm (annotated)</p>
--	--

— responsive reaction

Exhibit 2 to the Complaint.

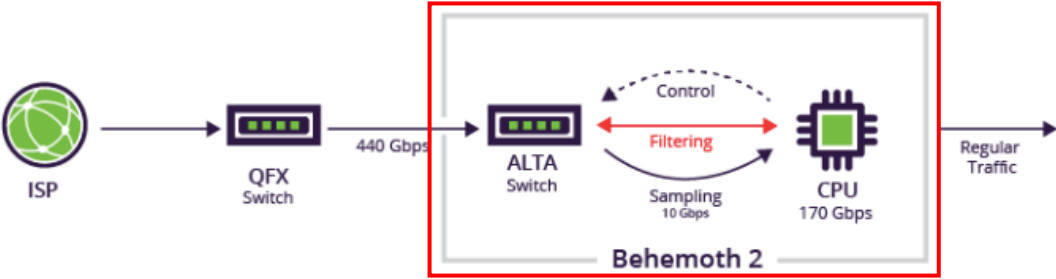
	 <p>In the new configuration, all traffic to the PoP is redirected to Behemoth 2.</p> <p>As shown in the figure, all the traffic entering the PoP is diverted to Behemoth 2, which will then apply internal sampling for DDoS detection. It also controls the Alta switch to divert the traffic for software mitigation. Alternatively, the mitigation service can install rules on the switch to perform the packet drop in hardware.</p> <p>Source: https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/</p>
<p>[20.P] A method of communicating a data unit through a computer communication network system, the</p>	<p>Imperva (“Company”) performs and induces others to perform a method of communicating a data unit through a computer communication network system.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, Company provides an Incapsula distributed denial-of-service (DDoS) protection service, that uses an Imperva Global Network to protect from DDoS attackers. Further, the network includes a multi-function point-of-presence (PoP), where each PoP is equipped with multiple Behemoths to prevent DDoS attacks and transfer the legitimate</p>

Exhibit 2 to the Complaint.


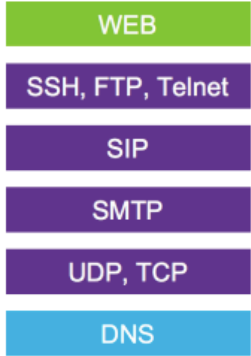
method comprising the following steps:	<p>traffic (“communicating a data unit”) from the various online assets such as Websites, DNS servers, SMTP servers and any other IP-based application (“computer communication network system”).</p> <div><div><p>INCAPSULA DDoS PROTECTION SERVICES</p><p>Name Server Protection</p><p>Website Protection</p><p>Infrastructure Protection</p></div><div><p>SERVER TYPES PROTECTED</p><p>WEB</p><p>SSH, FTP, Telnet</p><p>SIP</p><p>SMTP</p><p>UDP, TCP</p><p>DNS</p></div></div> <p>Source: http://www.ultris.com/documents/DDoS_Protection_DS.pdf, Page 3</p>
--	---

Exhibit 2 to the Complaint.

Incapsula Global Network

Unlike other services where DDoS was added to an existing content delivery network or web application firewall appliance, Incapsula designed a DDoS protection network from the ground up as an integral component of our comprehensive security and web acceleration solution. The Incapsula network fights the power of distributed attackers with an even greater distributed global defense. As the DDoS threat grows, so does the power of the Incapsula network. At the core of our network architecture is the multi-function PoP, distributed globally at strategic locations and served by major transit and hosting providers to ensure we remain close to your origin servers and end users. At the center of our DDoS mitigation capability is a purpose-built appliance that can manage up to 440 Gbps of traffic or 650 Mpps (millions of packets per second) – in fact, we call this The Behemoth. Each PoP is equipped with multiple Behemoths as well as WAF, bot protection, caching and load balancing services. The Incapsula network of PoPs continues to grow and can be seen on the [Incapsula network map](#).

Source: http://www.ultris.com/documents/DDoS_Protection_DS.pdf, Page 7

DDoS Protection for Networks can be used to protect any online asset such as websites, DNS servers, SMTP servers and any other IP based application. This service leverages Imperva's multi-terabit network capacity and packet processing capabilities to absorb and mitigate the largest and most sophisticated DDoS attacks.

DDoS Protection for Networks can be deployed as an always-on, on-demand or contingency solution, and can be combined with all Imperva Cloud Application Security services for extending protection and monitoring capabilities.

Source: <https://docs.imperva.com/bundle/cloud-application-security/page/introducing/network-ddos-protection.htm>

Exhibit 2 to the Complaint.

[20.1]
receiving, by
a gateway, a
first MPDU
from a
connection-
based
network of
the computer
communication network
system;

Company performs and induces others to perform a method of receiving, by a gateway, a first MPDU from a connection-based network of the computer communication network system.

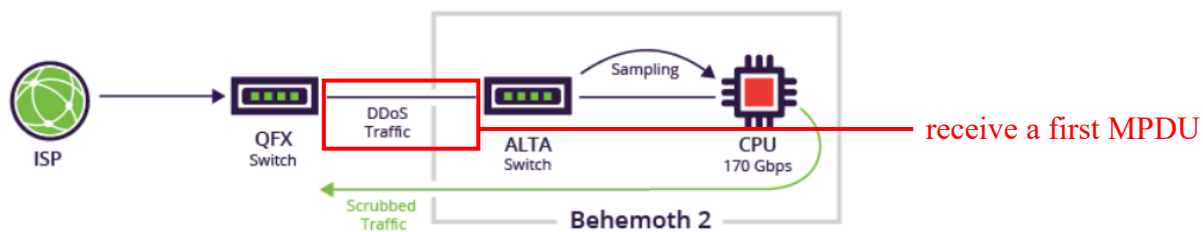
This element is infringed literally, or in the alternative, under the doctrine of equivalents.

For example, the Behemoth 2 (“gateway”) receives all traffic from the global network (“first MPDU”) that is further filtered using a filtering process to identify legitimate traffic and malicious traffic.



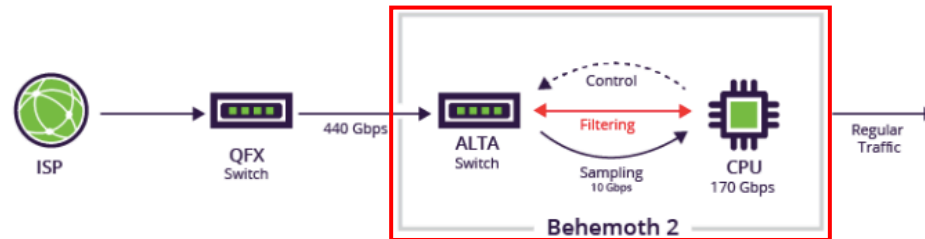
Behemoth 2

Source: <https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/> (annotated)



Source: <https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/> (annotated)

Exhibit 2 to the Complaint.



In the new configuration, all traffic to the PoP is redirected to Behemoth 2.

As shown in the figure, all the traffic entering the PoP is diverted to Behemoth 2, which will then apply internal sampling for DDoS detection. It also controls the Alta switch to divert the traffic for software mitigation. Alternatively, the mitigation service can install rules on the switch to perform the packet drop in hardware.

Source: <https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/>

3. Filtering—DDoS traffic is weeded out, usually by identifying patterns that instantly distinguish between legitimate traffic (i.e., humans, API calls and search engine bots) and malicious visitors. Responsiveness is a function of your being able to block an attack without interfering with your users' experience. The aim is for your solution to be completely transparent to site visitors.

Source: <https://www.imperva.com/learn/ddos/ddos-mitigation-services/>

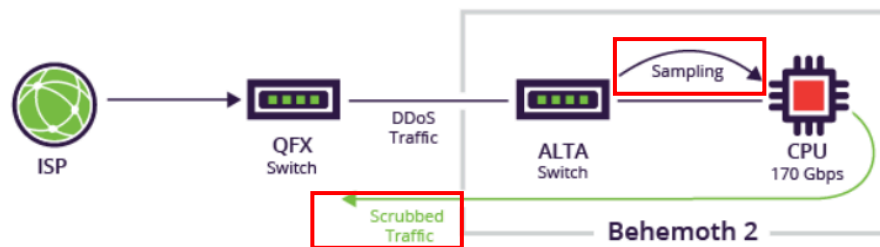
Exhibit 2 to the Complaint.

[20.2] disaggregating, by the gateway, the first MPDU into a plurality of smaller data units (DUs);

Company performs and induces others to perform a method of disaggregating, by the gateway, the first MPDU into a plurality of smaller data units (DUs).

This element is infringed literally, or in the alternative, under the doctrine of equivalents.

For example, after receiving all traffic from the global network, the Alta switch in Behemoth 2 performs the functioning of sampling and scrubbing where malicious packets are identified based on their header content, size, type, point of origin, etc. Therefore, it would be apparent to a person having ordinary skill in the art that the disaggregation of the first MPDU is done into a plurality of smaller data units (DUs) through sampling and scrubbing.

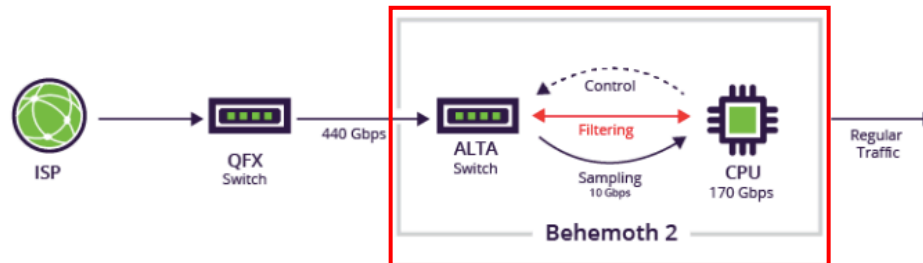


Source: <https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/>

- **Scrubbing**—an improvement on arbitrary sinkholing, scrubbing routes all ingress traffic through a security service. Malicious network packets are identified based on their header content, size, type, point of origin, etc. The challenge is to perform scrubbing at an inline rate without causing lag or otherwise impacting legitimate users.

Source: <https://www.imperva.com/learn/ddos/ddos-mitigation-services/>

Exhibit 2 to the Complaint.



In the new configuration, all traffic to the PoP is redirected to Behemoth 2.

As shown in the figure, all the traffic entering the PoP is diverted to Behemoth 2, which will then apply internal sampling for DDoS detection. It also controls the Alta switch to divert the traffic for software mitigation. Alternatively, the mitigation service can install rules on the switch to perform the packet drop in hardware.

Source: <https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/>

Exhibit 2 to the Complaint.

	<p>Single-stack speed, capacity, and accuracy</p> <p>Our high-capacity global network holds more than six Terabits per second (6 Tbps) of scrubbing capacity and can process more than 65 billion attack packets per second. This global network of 44+ points of presence (PoPs), each outfitted with a DDoS scrubbing center powered by proprietary Behemoth custom technology, cloud-based WAF, advanced bot mitigation services and more, acts as a software-defined mesh network for optimal performance. It scales as needed to absorb the largest attacks that can overwhelm legacy appliances. It also doesn't rely on a hybrid approach where failover to the cloud can mean the more persistent, small-scale attacks of today do damage before mitigation even starts. We incorporate crowdsourced learnings from emerging attack methods across our network, utilizing machine learning for the most up-to-date, accurate, and advanced protection.</p> <p>Source: https://www.imperva.com/resources/datasheets/Imperva_DDoS_Protection_20200730.pdf, Page 2</p>
<p>[20.3] collecting, by the gateway, selected network protocol data from the first MPDU, with the selected network protocol data including at least some network</p>	<p>Company performs and induces others to perform a method of collecting, by the gateway, selected network protocol data from the first MPDU, with the selected network protocol data including at least some network protocol data included in the first MPDU and not included in any of the plurality of DUs, and with the selected network protocol data relating exclusively to network protocols and including no data from any data payload(s) which may be present in the MPDU.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, the Alta switch in Behemoth 2 performs the function of filtering where the DDoS traffic is filtered by identifying patterns that instantly distinguish between legitimate traffic and malicious traffic (“selected network protocol data including at least some network protocol data included in the first MPDU and not included in any of the plurality of DUs”) to generate the scrubbed traffic.</p> <p>Furthermore, while sampling, different network-layer data packets such as UDP, and TCP are identified and mitigated to reduce the severity of the attack. Therefore, upon information and belief, mitigated UDP, and TCP data packets are</p>

Exhibit 2 to the Complaint.

<p>protocol data included in the first MPDU and not included in any of the plurality of DUs, and with the selected network protocol data relating exclusively to network protocols and including no data from any data payload(s) which may be present in the MPDU;</p>	<p>the selected network protocol data relating exclusively to network protocols and including no data from any data payload(s) that may be present in the MPDU.</p> <div data-bbox="531 362 1512 623"> </div> <p>In the new configuration, all traffic to the PoP is redirected to Behemoth 2.</p> <p>As shown in the figure, all the traffic entering the PoP is diverted to Behemoth 2, which will then apply internal sampling for DDoS detection. It also controls the Alta switch to divert the traffic for software mitigation. Alternatively, the mitigation service can install rules on the switch to perform the packet drop in hardware.</p> <p>Source: https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/</p> <div data-bbox="422 1166 1608 1386" style="border: 1px solid red; padding: 5px;"> <p>3. Filtering—DDoS traffic is weeded out, usually by identifying patterns that instantly distinguish between legitimate traffic (i.e., humans, API calls and search engine bots) and malicious visitors. Responsiveness is a function of your being able to block an attack without interfering with your users' experience. The aim is for your solution to be completely transparent to site visitors.</p> </div>
---	---

Exhibit 2 to the Complaint.

Source: <https://www.imperva.com/learn/ddos/ddos-mitigation-services/>

How it Works

Dedicated hardware is deployed in each of our PoPs to perform the stream processing required in order to collect statistics at network speed. Probabilistic data structures are used in conjunction with deterministic counting in order to provide reliable top statistics.

Analytics data is based on a 1:40 sampling resolution for DDoS traffic and a 1:1 sampling ratio for clean traffic, and data is collected in 15-second buckets.

Source: <https://www.imperva.com/blog/archive/enhanced-infrastructure-ddos-protection-analytics-targeted-visibility-for-greater-accuracy/>

Exhibit 2 to the Complaint.

What is a PPS or Network Protocol DDoS Attack?

An internet protocol is a discrete set of rules for exchanging information across the internet. TCP/IP is one of the most well-known rules for exchanging requests and data. A bad actor can severely disrupt an online service by exploiting these rules.

Protocol attacks often work at layers 3 and 4 of the OSI model on network devices like routers. Because they are on the network layer, they are measured in packets per second (pps).

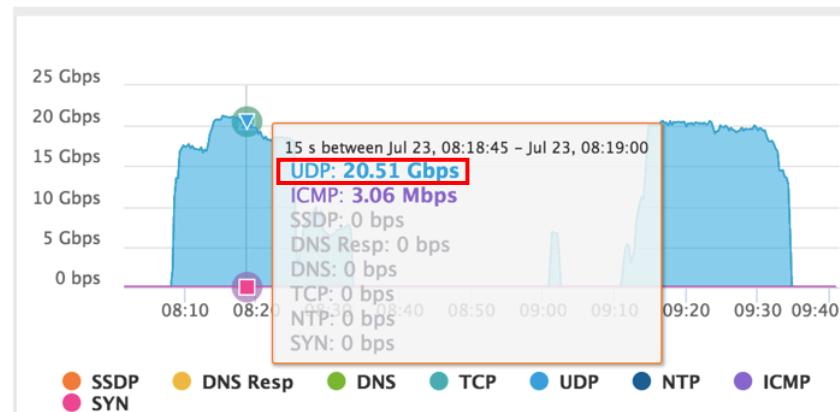
Below is a sampling of different network-layer DDoS attack types:

- UDP floods
- SYN floods
- NTP amplification
- DNS amplification
- SSDP amplification
- IP fragmentation
- SYN-ACK floods

Source: <https://www.imperva.com/learn/ddos/ddos-attacks/>

Exhibit 2 to the Complaint.

For a given range, we were able to display the size of the attack and the different attack vectors:



But other than the fact that we mitigated a lot of UDP traffic, it was impossible to dig deeper into the attack.

Source: <https://www.imperva.com/blog/archive/enhanced-infrastructure-ddos-protection-analytics-targeted-visibility-for-greater-accuracy/>

Support for any type of service

DDoS protection for networks supports any type of service, including TCP, UDP, SMTP, FTP, SSH, VoIP and proprietary or custom protocols.

Source: <https://www.imperva.com/products/infrastructure-ddos-protection-services/>

Exhibit 2 to the Complaint.

	<div data-bbox="420 280 802 323" data-label="Section-Header"> <h2>DDoS security policy</h2> </div> <div data-bbox="420 345 1625 446" data-label="Text"> <p>The traffic scrubbing that Imperva performs is based on a unique security policy that we define for each network range. The goal, of course, is to achieve the best granularity possible in order to minimize false positives and maximize mitigation.</p> </div> <div data-bbox="420 475 1642 644" data-label="Text"> <p>Imperva defines the security policy based on your traffic rates and patterns. When you first onboard your range to the DDoS for Networks service, we define an initial security policy according to our internal logic and the network information you provide in the scoping document. This information enables us to create an initial policy that allows a reasonable rate of traffic while blocking suspicious rates of traffic, until we have enough information to develop a more customized profile.</p> </div> <div data-bbox="420 672 1633 773" data-label="Text"> <p>After 7 days of traffic flow, the Imperva SD-SOC analyzes the data and automatically adjusts the security policy based on your network range's actual traffic patterns. Our Security Operations Center (SOC) reviews the policies as needed.</p> </div> <div data-bbox="420 812 764 852" data-label="Section-Header"> <h2>Mitigation process</h2> </div> <div data-bbox="420 875 1593 974" data-label="Text"> <p>The mitigation process built in to the Behemoth technology applies deep packet inspection combined with the application of advanced security rules and security challenges in order to identify malicious sources and/or content.</p> </div> <div data-bbox="420 1003 1585 1066" data-label="Text"> <p>Multiple mitigation steps are defined and evaluated independently for each traffic type, such as TCP, UDP, SYN, DNS, NTP, and so on.</p> </div> <div data-bbox="420 1097 1638 1198" data-label="Text"> <p>Each step is combined with thresholds in Kpps, Mbps, or both, in order to appropriately flag the traffic as malicious or legitimate. When the specified threshold is reached, the relevant mitigation step is activated. Mitigation steps are activated one at a time, as needed. Only the first and last steps are described here:</p> </div> <div data-bbox="405 1242 1797 1274" data-label="Text"> <p>Source: https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/security-policy.htm</p> </div>
--	--

Exhibit 2 to the Complaint.

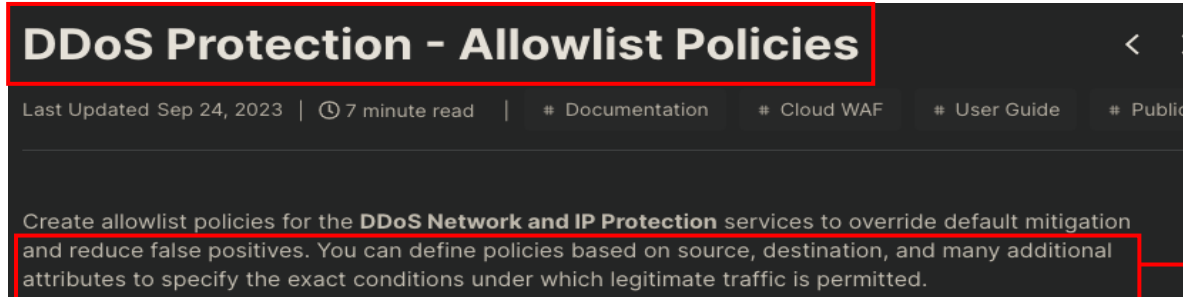
<p>[20.4] applying, by the gateway, a first rule to the selected network protocol data;</p>	<p>Company performs and induces others to perform a method of applying, by the gateway, a first rule to the selected network protocol data.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, Behemoth 2 applies the mitigation policies (“apply a first rule”) on the sampling data. The mitigation process built into the Behemoth technology applies deep packet inspection combined with the application of advanced security rules and security challenges to identify malicious sources and content. Multiple mitigation steps are defined and evaluated independently for each traffic type, such as TCP, UDP, SYN, DNS, and NTP.</p> <div data-bbox="407 607 1583 902">  <p>DDoS Protection - Allowlist Policies</p> <p>Last Updated Sep 24, 2023 7 minute read # Documentation # Cloud WAF # User Guide # Public</p> <p>Create allowlist policies for the DDoS Network and IP Protection services to override default mitigation and reduce false positives. You can define policies based on source, destination, and many additional attributes to specify the exact conditions under which legitimate traffic is permitted.</p> </div> <p>Source: https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/network-protection-policies.htm (annotated)</p>
---	---

Exhibit 2 to the Complaint.

	<div data-bbox="428 277 800 321" data-label="Section-Header"> <h2>DDoS security policy</h2> </div> <div data-bbox="428 342 1625 448" data-label="Text"> <p>The traffic scrubbing that Imperva performs is based on a unique security policy that we define for each network range. The goal, of course, is to achieve the best granularity possible in order to minimize false positives and maximize mitigation.</p> </div> <div data-bbox="428 472 1640 646" data-label="Text"> <p>Imperva defines the security policy based on your traffic rates and patterns. When you first onboard your range to the DDoS for Networks service, we define an initial security policy according to our internal logic and the network information you provide in the scoping document. This information enables us to create an initial policy that allows a reasonable rate of traffic while blocking suspicious rates of traffic, until we have enough information to develop a more customized profile.</p> </div> <div data-bbox="428 670 1633 776" data-label="Text"> <p>After 7 days of traffic flow, the Imperva SD-SOC analyzes the data and automatically adjusts the security policy based on your network range's actual traffic patterns. Our Security Operations Center (SOC) reviews the policies as needed.</p> </div> <div data-bbox="428 800 762 844" data-label="Section-Header"> <h2>Mitigation process</h2> </div> <div data-bbox="428 865 1591 974" data-label="Text"> <p>The mitigation process built in to the Behemoth technology applies deep packet inspection combined with the application of advanced security rules and security challenges in order to identify malicious sources and/or content.</p> </div> <div data-bbox="428 998 1583 1071" data-label="Text"> <p>Multiple mitigation steps are defined and evaluated independently for each traffic type, such as TCP, UDP, SYN, DNS, NTP, and so on.</p> </div> <div data-bbox="428 1096 1638 1200" data-label="Text"> <p>Each step is combined with thresholds in Kpps, Mbps, or both, in order to appropriately flag the traffic as malicious or legitimate. When the specified threshold is reached, the relevant mitigation step is activated. Mitigation steps are activated one at a time, as needed. Only the first and last steps are described here:</p> </div> <div data-bbox="415 1240 1791 1279" data-label="Text"> <p>Source: https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/security-policy.htm</p> </div>
--	---

Exhibit 2 to the Complaint.

	<div><div>Policy attributes</div><div>Use the following parameters to determine when the policy is applied.</div><div><div>Column</div><div>Filter results...</div><div>Q</div></div><table><thead><tr><th>ATTRIBUTE NAME</th><th>DESCRIPTION</th><th>SUPPORTED OPERATORS</th><th>ALLOWED VALUES</th></tr></thead><tbody><tr><td>Filter</td><td>Filter</td><td>Filter</td><td>Filter</td></tr><tr><td>IP protocol number (ip.proto)</td><td>The protocol number of the IP packet.</td><td>==</td><td>0-255</td></tr><tr><td>Source IP (ip.src)</td><td>The source IP address of the packet.</td><td>==,>=,<=,>,<</td><td>Subnet or single IP</td></tr></tbody></table><div>Source: https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/network-protection-policies.htm</div></div>	ATTRIBUTE NAME	DESCRIPTION	SUPPORTED OPERATORS	ALLOWED VALUES	Filter	Filter	Filter	Filter	IP protocol number (ip.proto)	The protocol number of the IP packet.	==	0-255	Source IP (ip.src)	The source IP address of the packet.	==,>=,<=,>,<	Subnet or single IP
ATTRIBUTE NAME	DESCRIPTION	SUPPORTED OPERATORS	ALLOWED VALUES														
Filter	Filter	Filter	Filter														
IP protocol number (ip.proto)	The protocol number of the IP packet.	==	0-255														
Source IP (ip.src)	The source IP address of the packet.	==,>=,<=,>,<	Subnet or single IP														
[20.5] selectively making, by the gateway, a responsive reaction based, at least in part, upon the application of the first rule	<p>Company performs and induces others to perform a method of selectively making, by the gateway, a responsive reaction based, at least in part, upon the application of the first rule to the selected network protocol data at the applying step.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p> <p>For example, Behemoth 2 blocks the suspicious traffic (“responsive reaction”) based on the selected policies applied by the device itself to the sampling data.</p>																

Exhibit 2 to the Complaint.

<p>to the selected network protocol data at the applying step; and</p>	<div data-bbox="415 272 804 316"> <h3>DDoS security policy</h3> </div> <div data-bbox="415 342 1652 443"> <p>The traffic scrubbing that Imperva performs is based on a unique security policy that we define for each network range. The goal, of course, is to achieve the best granularity possible in order to minimize false positives and maximize mitigation.</p> </div> <div data-bbox="415 475 1667 647"> <p>Imperva defines the security policy based on your traffic rates and patterns. When you first onboard your range to the DDoS for Networks service, we define an initial security policy according to our internal logic and the network information you provide in the scoping document. This information enables us to create an initial policy that allows a reasonable rate of traffic while blocking suspicious rates of traffic, until we have enough information to develop a more customized profile.</p> </div> <div data-bbox="415 680 1659 781"> <p>After 7 days of traffic flow, the Imperva SD-SOC analyzes the data and automatically adjusts the security policy based on your network range's actual traffic patterns. Our Security Operations Center (SOC) reviews the policies as needed.</p> </div> <div data-bbox="415 824 1936 885"> <p>Source: https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/security-policy.htm (annotated)</p> </div>
--	---

responsive
reaction

Exhibit 2 to the Complaint.

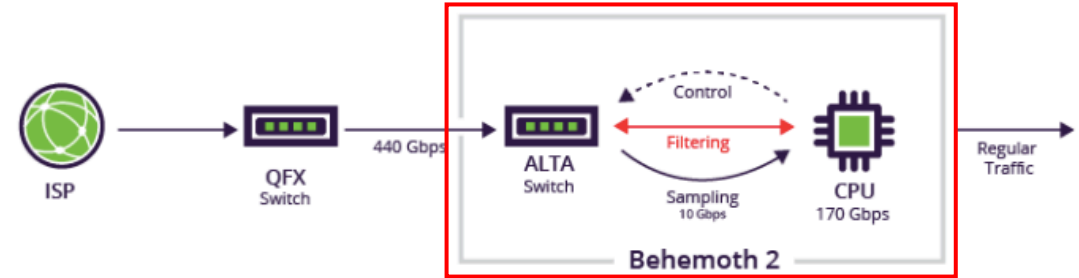
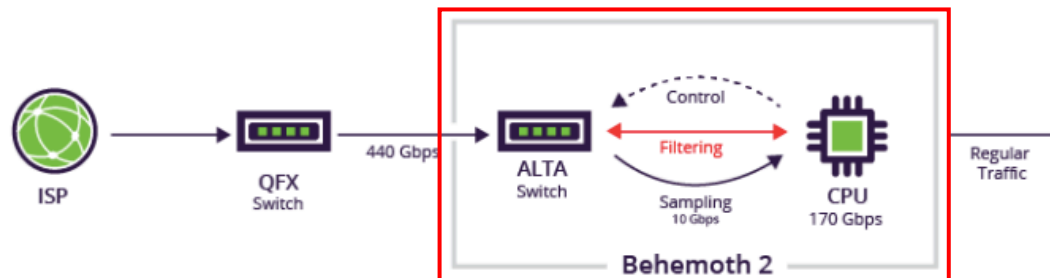
	 <p>In the new configuration, all traffic to the PoP is redirected to Behemoth 2.</p> <p>As shown in the figure, all the traffic entering the PoP is diverted to Behemoth 2, which will then apply internal sampling for DDoS detection. It also controls the Alta switch to divert the traffic for software mitigation. Alternatively, the mitigation service can install rules on the switch to perform the packet drop in hardware.</p> <p>Source: https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/</p>
<p>[20.6] selectively communicating, by the gateway, the first DU to a receiver-side connectionless network of</p>	<p>Company performs and induces others to perform a method of selectively communicating, by the gateway, the first DU to a receiver-side connectionless network of the computer communication network system on condition that the communicating of the first DU does not conflict with the responsive reaction of the selectively communicating step.</p> <p>This element is infringed literally, or in the alternative, under the doctrine of equivalents.</p>

Exhibit 2 to the Complaint.

<p>the computer communication network system on condition that the communication of the first DU does not conflict with the responsive reaction of the selectively communicating step.</p>	<p>For example, since the suspicious traffic is blocked, and the scrubbed traffic is transferred (“receiver side”), upon information and belief, the first DU which is in the form of scrubbed traffic is not blocked and is communicated without conflicting with the blocked traffic (“responsive reaction”) of the selectively communicating step.</p> <div data-bbox="415 407 1554 878"> <p>DDoS security policy</p> <p>The traffic scrubbing that Imperva performs is based on a unique security policy that we define for each network range. The goal, of course, is to achieve the best granularity possible in order to minimize false positives and maximize mitigation.</p> <p>Imperva defines the security policy based on your traffic rates and patterns. When you first onboard your range to the DDoS for Networks service, we define an initial security policy according to our internal logic and the network information you provide in the scoping document. This information enables us to create an initial policy that allows a reasonable rate of traffic while blocking suspicious rates of traffic, until we have enough information to develop a more customized profile.</p> <p>After 7 days of traffic flow, the Imperva SD-SOC analyzes the data and automatically adjusts the security policy based on your network range's actual traffic patterns. Our Security Operations Center (SOC) reviews the policies as needed.</p> </div> <p style="color: red; margin-left: 750px;">responsive reaction</p> <p>Source: https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/security-policy.htm (annotated)</p> <div data-bbox="415 1006 1730 1281"> <p>Imperva uses a GRE tunnel to route clean traffic to the origin (and also to establish BGP peering for on-demand DDoS Protection for Networks deployments).</p> <p>When Imperva advertises the customer's IPs or IP ranges, all packets targeted to these IPs/ranges are directed to the Imperva network. The Imperva Behemoth appliances scrub the traffic, filtering incoming packets and dropping any DDoS attack packets. The remaining “legitimate” packets are passed on to the customer according to their destination IP through the GRE tunnel.</p> </div> <p>Source: https://docs.imperva.com/bundle/cloud-application-security/page/introducing/network-ddos-protection.htm</p>
--	--

Exhibit 2 to the Complaint.



In the new configuration, all traffic to the PoP is redirected to Behemoth 2.

As shown in the figure, all the traffic entering the PoP is diverted to Behemoth 2, which will then apply internal sampling for DDoS detection. It also controls the Alta switch to divert the traffic for software mitigation. Alternatively, the mitigation service can install rules on the switch to perform the packet drop in hardware.

Source: <https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/>

Exhibit 2 to the Complaint.

2. List of References

1. http://www.ultris.com/documents/DDoS_Protection_DS.pdf, last accessed on 18 December 2023.
2. <https://docs.imperva.com/bundle/cloud-application-security/page/introducing/network-ddos-protection.htm>, last accessed on 18 December 2023.
3. <https://www.imperva.com/blog/archive/behemoth-2-mitigation-platform/>, last accessed on 18 December 2023.
4. https://www.imperva.com/resources/datasheets/Imperva_DDOS_Protection_20200730.pdf, last accessed on 18 December 2023.
5. <https://www.imperva.com/blog/archive/enhanced-infrastructure-ddos-protection-analytics-targeted-visibility-for-greater-accuracy/>, last accessed on 18 December 2023.
6. <https://www.imperva.com/learn/ddos/ddos-attacks/>, last accessed on 18 December 2023.
7. <https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/network-protection-policies.htm>, last accessed on 18 December 2023.
8. <https://www.imperva.com/learn/ddos/ddos-mitigation-services/>, last accessed on 18 December 2023.
9. <https://docs.imperva.com/bundle/cloud-application-security/page/network-ddos/security-policy.htm>, last accessed on 18 December 2023.
10. <https://www.imperva.com/products/infrastructure-ddos-protection-services/>, last accessed on 18 December 2023.